STATE OF MONTANA
DEPARTMENT OF CORRECTIONS
POLICY DIRECTIVE

Policy:	**DOC 1.7.13 OFFENDER ACCESS TO COMPUTERS**
Chapter 1:	ADMINISTRATION AND MANAGEMENT
Section 7:	Information Systems
Effective Date:	Dec. 1, 1996 Page 1 of 3
Revised:	12/07/2018
Signature:	/s/ Reginald D. Michael

I. POLICY

The Department of Corrections allows offenders controlled access to state-owned computers. This access is allowed for training, legal research, educational purposes, and as needed for work that offenders may perform in Department facilities and programs.

II. APPLICABILITY

All Department secure facilities.

III. DEFINITIONS

Administrator – The official, regardless of local title (division or facility administrator, bureau chief, warden, superintendent), ultimately responsible for the division, facility, or program operation and management.

Computer Peripherals – Any equipment that can be attached to a computer, including but not limited to: printers, monitors, scanners, digital cameras, and removable data storage media such as pen drives, DVD/CD drives, tape drives, and zip drives**.**

Freestanding Isolated Network – A group of computers networked only to each other. The freestanding isolated network will not have access to any other network.

Inmate Computer Network (ICON) – Department network that provides computer and resource access for inmate work and education programs.

Offender – Any individual in the custody of the Department of Corrections.

Password – An alphanumeric combination of characters unique to individual users that allow access to a specific computer, network or computer system.

Portable Electronic Storage Media (Portable Storage) – Includes floppy disks, CDs, DVDs, optical platters, flash memory drives, backup tapes, external hard drives, and other electronic storage media or devices that provide portability or mobility of data.

Server – A computer that serves programs, files, and printing services to other computers on the network.

Stand-Alone Computer – A computer that is not attached to any network.

User ID – Used generically to refer to CI number, login ID, user account, or any other term used to describe a user's unique identifier which is used to grant rights and privileges on a computer, computer system or network. User IDs are never reused.

IV. DEPARTMENT DIRECTIVES

A. Prohibitions

1. Under no circumstances will facilities allow any offender to access:
   a. the internet on unapproved or staff use systems;
   b. e-mail; or
   c. unapproved or non-offender computers or servers;

2. Under no circumstances will facilities allow offenders to save or maintain personal files on a state owned computer or server.

3. Any unauthorized inmate use of a state owned computer is strictly prohibited.

B. Computer Labeling

1. Each facility will:
   a. conspicuously label all computers and peripherals, which are located in offender-accessible areas, with a laminated card, designating them as either *Offender Use* or *Staff Use Only* to ensure visual identification;
   b. permit offenders to only access computers labeled *Offender Use;* and
   c. ensure the laminated card attached to each *Offender Use* computer includes all authorized programs allowed on that specific computer.

C. Offender Access to Stand Alone Computers or Free Standing Isolated Networks

1. The work area supervisor may allow an offender to access stand-alone computers and freestanding isolated networks; however, the computers must be labeled as outlined in Section IV.B above.

2. The administrator and CIO must approve in writing the creation of any new, free-standing, isolated networks.

D. Offender Access to ICON

1. The Administrative Services Division Network Services Bureau, in conjunction with the Department of Administration's Information Technology Services Division, will manage ICON.

2. Each facility/program will designate staff to manage the offender accounts for access to work or educational computers.

3. Each facility/program with inmates utilizing ICON will create a process for authorizing offender access. All offender access to any offender use system will be provided for through the facility/program inmate access procedure.

4. Once an offender is approved for ICON access, the designated facility/program staff will assign the offender the appropriate rights on ICON. The offender's User ID will be their OMIS DOC ID.

5. When an offender leaves a job assignment, the work area supervisor must notify the designated facility/program staff to remove the offender from ICON access.

6. When an offender leaves a classroom assignment, the instructor must notify the designated facility/program staff to remove the offender from ICON access.

7. At no time will an offender use network credentials (user ID and password) other than their own or provide another offender their credentials. Violations will result in disciplinary action in accordance with *DOC 3.4.1 Offender Disciplinary System* and facility disciplinary procedures.

E. Offender Access to Peripherals and Disks

1. Each facility/program will ensure that offender access to peripherals is limited and closely supervised.

2. Each facility/program will develop specific procedures regarding the use of all peripherals. In the case of scanners and digital cameras, the supervisor must review and approve the project in writing prior to allowing the offender access to the equipment.

3. Supervisors may allow offenders to use portable electronic storage media for appropriate work-related assignments and educational programs in coordination with Department policies and procedures and the area supervisor.

4. Under no circumstances will supervisors allow offenders to move portable electronic storage media from their assigned work area to another area without staff approval.

5. Possession of portable electronic storage media in offender living areas or use of disks for personal needs is strictly prohibited. Violations will result in disciplinary action in accordance with *DOC 3.4.1 Offender Disciplinary System* and facility disciplinary procedures.

V. CLOSING

Questions concerning this policy should be directed to the Administrative Services Division Administrator.

VI. REFERENCES

A. 2-15-112, MCA; 2-15-114, MCA; 53-1-203, MCA
B. Montana Operations Manual – Information Security Policy

VII. ATTACHMENTS

None.